Corrigé DS n° 1

Ⓐ 1. • $(\mathbb{H},+)$ est un groupe : c'est le groupe produit de $(\mathbb{C},+)$ par lui-même

• $\times$ est interne ds $\mathbb{H}$

$\times$ associative : $\forall (z_1,z_2)\,(z'_1,z'_2)\,(z''_1,z''_2) \in \mathbb{H}$ $\quad (z_1,z_2)\times[(z'_1,z'_2)\times(z''_1,z''_2)]$

$$= [(z_1,z_2)\times(z'_1,z'_2)]\times(z''_1,z''_2)$$

(voir calculs à l'aide de Maple ci-dessous)

$\times$ admet un él^t neutre : $(1,0)$: $\forall (z_1,z_2)\in\mathbb{H}$ $\quad (1,0)\times(z_1,z_2) = (z_1,z_2)\times(1,0) = (z_1,z_2)$

$\times$ distributive à droite et à gauche p.r. à $+$: là encore, laissons Maple faire les calculs...

Tout cela montre que <u>$(\mathbb{H},+,\times)$ est un anneau</u> ; cet anneau n'est pas commutatif (par ex. $(i,0)\times(0,1) \neq (0,1)\times(i,0)$)

```
> restart;
> multq:=proc(q1,q2);
> RETURN([q1[1]*q2[1]-q1[2]*conjugate(q2[2]),
          q1[1]*q2[2]+q1[2]*conjugate(q2[1])])
  end:
> q1:=[z1,z2]:q2:=[z3,z4]:q3:=[z5,z6]:
> multq(q1,multq(q2,q3))-multq(multq(q1,q2),q3);
```

$$[-(z1\,z3 - z2\,\overline{z4})\,z5 + (z1\,z4 + z2\,\overline{z3})\,\overline{z6} + z1\,(z3\,z5 - z4\,\overline{z6}) - z2\,\overline{z3\,z6 + z4\,\overline{z5}},$$
$$-(z1\,z3 - z2\,\overline{z4})\,z6 - (z1\,z4 + z2\,\overline{z3})\,\overline{z5} + z1\,(z3\,z6 + z4\,\overline{z5}) + z2\,\overline{z3\,z5 - z4\,\overline{z6}}]$$

```
> simplify(expand(expand(")));
```

$$[0, 0]$$

```
> multq(q1,q2+q3)-multq(q1,q2)-multq(q1,q3);
```

$$[-z1\,z5 + z2\,\overline{z6} - z1\,z3 + z2\,\overline{z4} + z1\,(z5 + z3) - z2\,\overline{z6 + z4},$$
$$-z1\,z6 - z2\,\overline{z5} - z1\,z4 - z2\,\overline{z3} + z1\,(z6 + z4) + z2\,\overline{z5 + z3}]$$

```
> simplify(expand("));
```

$$[0, 0]$$

2\. a) φ morphisme d'anneaux : il suffit de vérifier : $\varphi(1_{\mathbb{R}}) = 1_{\mathbb{H}}$, et,

$\forall (x,y)\in\mathbb{R}^2 \quad \varphi(xy) = \varphi(x)\varphi(y)$, $\varphi(x+y) = \varphi(x)+\varphi(y)$.

φ est injectif car : $\forall (x,y)\in\mathbb{R}^2$ $\quad \varphi(x) = \varphi(y) \Rightarrow (x,0) = (y,0) \Rightarrow x = y$.

b) Soit $q = (z_1,z_2)\in\mathbb{H}$ et $x\in\mathbb{R}$. Alors $\quad xq = qx = (xz_1, xz_2)$

c) • Soient $x_0,x_1,x_2,x_3\in\mathbb{R}$. Alors, d'après le calcul ci-dessus, on a :

$x_0e_0 = (x_0,0)$ $\quad x_1e_1 = (ix_1,0)$ $\quad x_2e_2 = (0,x_2)$ et $x_3e_3 = (0,ix_3)$.

d'où $\displaystyle\sum_{i=0}^{3} x_ie_i = (x_0+ix_1,\, x_2+ix_3)$

Or tout $q \in \mathbb{H}$ s'écrit justement de façon unique sous la forme (x_0+ix_1, x_2+ix_3) avec x_i réels, d'où le résultat demandé.

- Un quaternion est réel ssi il est de la forme $(x_0, 0)$ avec x_0 réel, i.e. si et seul^{t} si $x_1 = x_2 = x_3 = 0$.

d) On a le tableau suivant :

$\times$	e_0	e_1	e_2	e_3
e_0	e_0	e_1	e_2	e_3
e_1	e_1	$-e_0$	e_3	$-e_2$
e_2	e_2	$-e_3$	$-e_0$	e_1
e_3	e_3	e_2	$-e_1$	$-e_0$

On en déduit alors facilement :

$$\sum_{i=0}^{3} x_i e_i \times \sum_{i=0}^{3} y_i e_i = (x_0y_0 - x_1y_1 - x_2y_2 - x_3y_3)e_0 + (x_0y_1 + x_1y_0 + x_2y_3 - x_3y_2)e_1$$
$$+ (x_0y_2 + x_2y_0 + x_3y_1 - x_1y_3)e_2 + (x_0y_3 + x_3y_0 + x_1y_2 - x_2y_1)e_3.$$

e) Le calcul précédent montre facilement qu'un quaternion $q = \sum_{i=0}^{3} x_i e_i$ $(x_i \in \mathbb{R})$ commute avec tous les autres si et seul^{t} si : $\begin{cases} x_2y_3 = x_3y_2 \\ x_3y_1 = x_1y_3 \\ x_1y_2 = x_2y_1 \end{cases}$ pour <u>tous</u> $(y_1, y_2, y_3) \in \mathbb{R}^3$

On en déduit facilement $x_1 = x_2 = x_3 = 0$ d'où q réel. Réciproque déjà faite au b).

---

3). Si $\lambda \in \mathbb{R}$, on a $\lambda . q = (\lambda, 0) \times q = \lambda \times q$ (calcul déjà fait au 2.b)

- $(\mathbb{H}, +, .)$ est un $\mathbb{R}$-espace vectoriel : c'est l'espace vectoriel produit de $(\mathbb{C}, +, .)$ par lui-même.
- $(\mathbb{H}, +, \times, .)$ est une $\mathbb{R}$-algèbre car de plus : $\forall \lambda \in \mathbb{R}$, $\forall q, q' \in \mathbb{H}$
  $(\lambda . q)q' = (\lambda q)q' = (q\lambda)q' = q(\lambda . q') = \lambda . (qq')$ (car λ réel commute avec q)
- D'après 2c), (e_0, e_1, e_2, e_3) base de $\mathbb{H}$ donc $\dim_{\mathbb{R}} \mathbb{H} = 4$.

---

4) a) facile

b) Un calcul simple montre : $\forall \lambda \in \mathbb{R}$, $\forall (q, q') \in \mathbb{H}^2$ $\overline{\lambda q + \mu q'} = \lambda \bar{q} + \mu \bar{q}'$

donc l'application $\varphi : q \mapsto \bar{q}$ est un ~~endomorphisme~~ de l'e.v. $(\mathbb{H}, +, .)$.

De plus, $\varphi \circ \varphi = id_{\mathbb{H}}$ (φ est involutive), donc φ est bijective (et $\varphi^{-1} = \varphi$).

c) $\overline{qq'} = \bar{q}' \bar{q}$: il suffit de calculer... Pour cela, il était astucieux de remarquer que, si $q = (z_1, z_2)$ $\bar{q} = (\bar{z}_1, -z_2)$ donc :

si $q = (z_1, z_2)$ et $q' = (z'_1, z'_2)$ $\overline{qq'} = (\overline{z_1 z'_1 - z_2 \bar{z}'_2}, -z_1 z'_2 - z_2 \bar{z}'_1)$

et $\bar{q}'\bar{q} = (\bar{z}'_1, -z'_2) \times (\bar{z}_1, -z_2) = (\bar{z}'_1 \bar{z}_1 - z'_2 \bar{z}_2, -\bar{z}'_1 z_2 - z'_2 \bar{\bar{z}}_1)$

d'où le résultat.

d) Si $q = (z_1, z_2)$, alors $q\bar{q} = (z_1, z_2) \times (\bar{z}_1, -z_2) = (|z_1|^2 + |z_2|^2, 0)$ donc $N(q) = |z_1|^2 + |z_2|^2$ est un réel positif et $N(q) = 0 \iff z_1 = z_2 = 0 \iff q = 0$.

e) $N(qq') = qq'\overline{qq'} = qq'\bar{q}'\bar{q} = q\,N(q')\bar{q} = N(q)q\bar{q} = N(q)N(q')$ (car $N(q)$ réel donc commute avec ts les quaternions)

En échangeant les rôles de q' et q, on obtient $N(qq') = N(q'q) = N(q)N(q')$.

f) si $q \neq 0$, $N(q) \neq 0$ et $q \cdot \dfrac{\bar{q}}{N(q)} = 1$. De même $\dfrac{\bar{q}}{N(q)} \cdot q = 1$ (car $\bar{q}q = N(\bar{q}) = N(q)$)

donc q est inversible, d'inverse $\dfrac{\bar{q}}{N(q)}$.

Tout élt non nul de $\mathbb{H}$ est donc inversible : $(\mathbb{H}, +, \times)$ est un corps.

---

5) a) Si $q = (z_1, z_2)$: $q = \bar{q} \Leftrightarrow (z_1, z_2) = (\bar{z}_1, -z_2) \Leftrightarrow z_1$ réel et $z_2 = 0 \Leftrightarrow q \in \mathbb{R}$.

$q = -\bar{q} \Leftrightarrow (z_1, z_2) = (-\bar{z}_1, z_2) \Leftrightarrow z_1$ imaginaire pur et z_2 quelc. $\Leftrightarrow q \in \mathbb{P}$.

b) Si $q \in \mathbb{R}$, alors $q^2 \in \mathbb{R}_+$: évident.

Récip., si $q^2 \in \mathbb{R}_+$ alors il existe $x \in \mathbb{R}$ tq $q^2 = x^2$, soit $q^2 - x^2 = 0$

soit $(q-x)(q+x) = 0$ d'où $q = \pm x$ car $\mathbb{H}$ est un corps. Ainsi, $q \in \mathbb{R}$.

c) • Soient $a, b \in \mathbb{R}$, avec $a \neq q + \bar{q}$, tq $q^2 - aq + b = 0$. Alors $\overline{q^2 - aq + b} = 0$ soit

$\bar{q}^2 - a\bar{q} + b = 0$ (car l'appl. $q \mapsto \bar{q}$ est un morphisme d'e.v).

On en déduit, en soustrayant les 2 relations : $\bar{q}^2 - q^2 = a(\bar{q} - q)$ d'où $q = \bar{q}$ (car $a \neq q + \bar{q}$) i.e. $q \in \mathbb{R}$.

• Soit $q \in \mathbb{P}$: $q = (ix_1, z_2)$ avec $x_1 \in \mathbb{R}$ d'où $q^2 = (-x_1^2 - |z_2|^2, 0) \in \mathbb{R}_-$

• Soit $q \in \mathbb{H}$ tel que $q^2 \in \mathbb{R}_-$

- soit $q^2 = 0$ et, dans ce cas, $q = 0 \in \mathbb{P}$
- soit $q^2 < 0$: alors $q \notin \mathbb{R}$ (car d'après (b), $q \in \mathbb{R}^* \Rightarrow q^2 > 0$)

et q est solution de l'équation $q^2 + b = 0$ (avec $b = -q^2 \in \mathbb{R}$). D'après ce qui précède, on en déduit $a = q + \bar{q} = 0$ soit $q \in \mathbb{P}$. cqfd

---

(B) 1) On montre que $(\mathrm{Aut}(\mathbb{H}), \circ)$ est un sous-groupe du groupe $(\Sigma(\mathbb{H}), \circ)$ des permutations de $\mathbb{H}$. Pour cela :

• $\mathrm{Aut}(\mathbb{H}) \neq \emptyset$ car $id_{\mathbb{H}} \in \mathrm{Aut}(\mathbb{H})$

• Si $\sigma_1, \sigma_2 \in \mathrm{Aut}(\mathbb{H})$, alors $\sigma_1 \circ \sigma_2 \in \mathrm{Aut}(\mathbb{H})$ car :

$\forall (x,y) \in \mathbb{H}^2$: $\sigma_1 \circ \sigma_2(1_{\mathbb{H}}) = \sigma_1(1) = 1$

$\sigma_1 \circ \sigma_2(x+y) = \sigma_1[\sigma_2(x) + \sigma_2(y)] = \sigma_1 \circ \sigma_2(x) + \sigma_1 \circ \sigma_2(y)$

$\sigma_1 \circ \sigma_2(xy) = \sigma_1[\sigma_2(x)\sigma_2(y)] = \sigma_1 \circ \sigma_2(x) \times \sigma_1 \circ \sigma_2(y)$

• Si $\sigma \in \mathrm{Aut}(\mathbb{H})$ alors $\sigma^{-1} \in \mathrm{Aut}(\mathbb{H})$ car :

- $\sigma^{-1}(1) = \sigma^{-1}(\sigma(1)) = 1$
- si $x', y' \in \mathbb{H}$, $x' = \sigma(x)$ $y' = \sigma(y)$ (car σ bij. de $\mathbb{H} \to \mathbb{H}$)

et $\sigma^{-1}(x'+y') = \sigma^{-1}(\sigma(x) + \sigma(y)) = \sigma^{-1}(\sigma(x+y)) = x + y = \sigma^{-1}(x') + \sigma^{-1}(y')$

et, de même, $\sigma^{-1}(x'y') = \sigma^{-1}(x') \times \sigma^{-1}(y')$.

2) b) Soit $x \in \mathbb{R}$. Alors, d'après A.2.e : $\forall q \in \mathbb{H}\quad qx = xq$ d'où $\sigma(q)\sigma(x) = \sigma(x)\sigma(q)$

Or, σ étant bijective, tout quaternion $q' \in \mathbb{H}$ peut s'écrire $q' = \sigma(q)$ d'où :

$$\forall q' \in \mathbb{H},\quad q'.\sigma(x) = \sigma(x).q'.$$

Ainsi, $\sigma(x)$ commute avec tous les quaternions, d'où $\sigma(x) \in \mathbb{R}$ d'après A.2.e.

On a donc bien $\underline{\sigma(\mathbb{R}) \subset \mathbb{R}}$.

a) c) d) : cf exercice corrigé en classe (feuille n° 1), puisque, d'après la question ci-dessus, $\sigma|_{\mathbb{R}}$ est un automorphisme du corps $\mathbb{R}$.

e) Soit $q \in \mathbb{P}$. Alors : $[\sigma(q)]^2 = \sigma(q^2)$. Or $q^2 \in \mathbb{R}_-$ et $\sigma(\mathbb{R}_-) \subset \mathbb{R}_-$ (car $\sigma|_{\mathbb{R}}$ est croissante et $\sigma(0) = 0$). Donc $\sigma(q^2) \in \mathbb{R}_-$ et d'après A.5.c, $\underline{\sigma(q) \in \mathbb{P}}$.

f) • Si $q \in \mathbb{H}$: $q + \bar{q} \in \mathbb{R}$ donc $\sigma(q+\bar{q}) = \sigma(q) + \sigma(\bar{q}) \in \mathbb{R}$ d'après b)

$q - \bar{q} \in \mathbb{P}$ donc $\sigma(q-\bar{q}) = \sigma(q) - \sigma(\bar{q}) \in \mathbb{P}$ d'après e)

• On a donc : $\overline{\sigma(q)+\sigma(\bar{q})} = \sigma(q) + \sigma(\bar{q})$ et $\overline{\sigma(q) - \sigma(\bar{q})} = -(\sigma(q) - \sigma(\bar{q}))$

D'où $\overline{\sigma(q)+\sigma(\bar{q})} + \overline{\sigma(q)-\sigma(\bar{q})} = 2\,\overline{\sigma(q)} = 2\sigma(\bar{q})$. D'où $\underline{\sigma(\bar{q}) = \overline{\sigma(q)}}$

• On en déduit : $N(\sigma(q)) = \sigma(q)\overline{\sigma(q)} = \sigma(q)\sigma(\bar{q}) = \sigma(q\bar{q}) = \sigma(N(q)) = N(q)$ (car $N(q) \in \mathbb{R}$).

---

3) a) Soit $\varphi_a : q \longmapsto aqa^{-1}$ $(a \neq 0)$. On a : $\varphi_a(1_{\mathbb{H}}) = 1_{\mathbb{H}}$ et

$$\forall (x,y) \in \mathbb{H}^2 \quad \varphi_a(x+y) = a(x+y)a^{-1} = axa^{-1} + aya^{-1} = \varphi_a(x) + \varphi_a(y)$$

$$\varphi_a(xy) = axya^{-1} = axa^{-1}aya^{-1} = \varphi_a(x)\varphi_a(y)$$

donc $\underline{\varphi_a \text{ morphisme du corps } \mathbb{H}}$.

De plus : $\forall y \in \mathbb{H}$, $y = \varphi_a(x) \iff y = axa^{-1} \iff x = a^{-1}ya$, donc φ_a est bijective (et $(\varphi_a)^{-1} = \varphi_{a^{-1}}$). Donc $\underline{\varphi_a \in \mathrm{Aut}(\mathbb{H})}$

b) • On vérifie facilement $\Phi(ab) = \varphi_a \circ \varphi_b = \Phi(a) \circ \Phi(b)$, donc Φ est un morphisme du groupe $(\mathbb{H}\setminus\{0\}, \times)$ dans le groupe $(\mathrm{Aut}(\mathbb{H}), \circ)$

• Son noyau est l'ensemble des $a \in \mathbb{H}\setminus\{0\}$ tq $\Phi(a) = 1_{\mathrm{Aut}(\mathbb{H})} = id_{\mathbb{H}}$

Or $\varphi_a = id_{\mathbb{H}} \iff \forall q \in \mathbb{H}\ aqa^{-1} = q \iff \forall q \in \mathbb{H}\ aq = qa \iff a$ réel (d'après A.2.e)

Donc : $\underline{\mathrm{Ker}\,\Phi = \mathbb{R}^*}$

---

4) a) $[\sigma(e_1)]^2 = \sigma(e_1^2) = \sigma(-1) = -1$

b) • $(\sigma(e_1)e_1 - 1)e_1 = \sigma(e_1)e_1^2 - e_1 = -\sigma(e_1) - e_1$

$\sigma(e_1)(\sigma(e_1)e_1 - 1) = \sigma(e_1)^2 e_1 - \sigma(e_1) = -e_1 - \sigma(e_1)$

d'où l'égalité demandée

• Si $\sigma(e_1)e_1 - 1 \neq 0$, il est inversible dans $\mathbb{H}$ donc l'égalité précédente s'écrit

$$e_1 = (\sigma(e_1)e_1 - 1)^{-1}\,\sigma(e_1)\,(\sigma(e_1)e_1 - 1) = a\,\sigma(e_1)\,a^{-1} = \varphi_a \circ \sigma(e_1)$$

avec $\underline{a = (\sigma(e_1)e_1 - 1)^{-1}}$

c) si $\sigma(e_1)e_1 = 1$ alors $\sigma(e_1) = e_1^{-1} = e_1$. Or $e_2\sigma(e_1)e_2^{-1} = e_2(-e_1)(-e_2) = e_2e_3 = e_1$

soit $e_1 = \varphi_a \circ \sigma(e_1)$ avec $\underline{a = e_2}$.

---

5) a) . On a $\sigma'(e_1) = \varphi_a \circ \sigma(e_1) = e_1$ d'où

$$\sigma'(e_1)(\sigma'(e_2)e_2 - 1) = \sigma'(e_1)\sigma'(e_2)e_2 - \sigma'(e_1) = \sigma'(e_1e_2)e_2 - \sigma'(e_1) = \sigma'(-e_2e_1)e_2 - \sigma'(e_1)$$
$$= -\sigma'(e_2)\sigma'(e_1)e_2 - \sigma'(e_1) = -\sigma'(e_2)e_1e_2 - e_1 = \sigma'(e_2)e_2e_1 - e_1$$
$$= (\sigma'(e_2)e_2 - 1)e_1$$

(on a utilisé le fait que σ', composé d'automorphismes de $\mathbb{H}$, est aussi un automorphisme).

. On en déduit, si $\sigma'(e_2)e_2 \neq 1$: $(\sigma'(e_2)e_2 - 1)^{-1}\sigma'(e_1)(\sigma'(e_2)e_2 - 1) = e_1$

soit $\varphi_b \circ \sigma'(e_1) = e_1$ avec $b = (\sigma'(e_2)e_2 - 1)^{-1}$.

On a également $\varphi_b \circ \sigma'(e_2) = e_2$ car :

$$\varphi_b \circ \sigma'(e_2) = (\sigma'(e_2)e_2 - 1)^{-1}\sigma'(e_2)(\sigma'(e_2)e_2 - 1)$$
$$= (\sigma'(e_2)e_2 - 1)^{-1}([\sigma'(e_2)]^2 e_2 - \sigma'(e_2))$$
$$= (\sigma'(e_2)e_2 - 1)^{-1}(-e_2 - \sigma'(e_2)) \quad (\text{car } [\sigma'(e_2)]^2 = \sigma'(e_2^2) = \sigma'(-1) = -1)$$
$$= (\sigma'(e_2)e_2 - 1)^{-1}(-1 + \sigma'(e_2)e_2)e_2 = e_2$$

donc $\underline{b = (\sigma'(e_2)e_2 - 1)^{-1}}$ convient

b) si $\sigma'(e_2)e_2 = 1$, $\sigma'(e_2) = e_2^{-1} = -e_2$. On vérifie alors facilement que $b = e_1$ convient

---

6) a) $\sigma'' = \varphi_b \circ \varphi_a \circ \sigma$ est un automorphisme de $\mathbb{H}$. On a :

$$\sigma''(e_3) = \sigma''(e_1e_2) = \sigma''(e_1)\sigma''(e_2) = e_1e_2 = e_3 \quad \left(\begin{array}{l}\sigma''(e_1) = \varphi_b \circ \sigma'(e_1) = e_1 \\ \sigma''(e_2) = \varphi_b \circ \sigma'(e_2) = e_2\end{array}\right)$$

b) On a également $\sigma''(e_0) = e_0$ (car $e_0 = 1$)

Donc, pour $\forall q \in \mathbb{H}$, $q = \sum_{i=0}^{3} x_i e_i$ ($x_i \in \mathbb{R}$), on a : $\sigma''(q) = \sum \sigma''(x_i e_i) = \sum \sigma''(x_i)\sigma''(e_i)$
$= \sum x_i e_i$

($\sigma''(x_i) = x_i$ car x_i réel)

soit $\sigma''(q) = q$: $\sigma'' = id_{\mathbb{H}}$.

Par suite $\varphi_b \circ \varphi_a \circ \sigma = id_{\mathbb{H}}$ soit $\sigma = (\varphi_b \circ \varphi_a)^{-1} = \varphi_a^{-1} \circ \varphi_b^{-1} = \varphi_{a^{-1}} \circ \varphi_{b^{-1}} = \varphi_{a^{-1}b^{-1}}$

soit $\sigma = \Phi(a^{-1}b^{-1}) \longrightarrow$ <u>Φ surjective</u>.

PARTIE D

2) a) Un élt de $\mathbb{W}$ s'écrit sous la forme : $q \in \mathbb{H}(\mathbb{Z})$ ou $q + \varepsilon$, avec $q \in \mathbb{H}(\mathbb{Z})$, et en posant $\varepsilon = \frac{1 + e_1 + e_2 + e_3}{2}$

. Or : $\forall q, q' \in \mathbb{H}(\mathbb{Z})$ $q + q' \in \mathbb{H}(\mathbb{Z})$ et $qq' \in \mathbb{H}(\mathbb{Z})$.

. Pour vérifier que $\mathbb{W}$ est stable par addition (évident) et multiplication, il suffit donc de vérifier que : $\forall q \in \mathbb{H}(\mathbb{Z})$, $\varepsilon q \in \mathbb{W}$, $q\varepsilon \in \mathbb{W}$ et $\varepsilon^2 \in \mathbb{W}$

Or : - $\varepsilon^2 = \varepsilon - 1 \in W$

- si $q = x_0e_0 + x_1e_1 + x_2e_2 + x_3e_3$ avec $x_i \in \mathbb{Z}$, un calcul rapide montre que εq et $q\varepsilon$ sont aussi éléments de W

• Enfin, il est clair que $1 \in W$, donc, finalement, W est un sous-anneau de $\mathbb{H}$.

b) Vérification facile -

c) • Soit $q \in W$. Si $N(q) = 1$, alors $q\bar{q} = 1$. Donc $\bar{q}$ est l'inverse de q, et il est facile de vérifier que $\bar{q} \in W$. Donc q est inversible dans W

• Réciproquement, si $q \in W$ est inversible dans W, il existe $q' \in W$ tel que $qq' = q'q = 1$. Et on a alors $N(q)N(q') = 1$. Or $N(q) \in \mathbb{N}$, $N(q') \in \mathbb{N}$. On en déduit donc $N(q) = 1$.

d) • Soit $q \in \mathbb{H}(\mathbb{Q})$, $q = q_0 + q_1e_1 + q_2e_2 + q_3e_3$ avec $q_i \in \mathbb{Q}$.

Pour tout réel x, on a : $E(x+\frac{1}{2}) \leq x + \frac{1}{2} < E(x+\frac{1}{2}) + 1$ donc $-\frac{1}{2} \leq x - E(x+\frac{1}{2}) < \frac{1}{2}$

De plus, $x + \frac{1}{2} = E(x+\frac{1}{2})$ si et seulement si $x \in \frac{1}{2} + \mathbb{Z}$.

Donc : • si l'un des q_i n'appartient pas à $\frac{1}{2} + \mathbb{Z}$, posons $a_i = E(q_i + \frac{1}{2})$

On a alors $|q_i - a_i| \leq \frac{1}{2}$ pour tout i, et $|q_i - a_i| < \frac{1}{2}$ pour un i au moins.

On aura alors $N(q-a) = \sum_{i=0}^{3}(q_i - a_i)^2 < 1$, avec $a \in \mathbb{H}(\mathbb{Z})$

• si tous les q_i appartiennent à $\frac{1}{2} + \mathbb{Z}$, posons $a = q$. Alors $a \in W$, et $N(q-a) = 0 < 1$.

• Soit $a, q \in W$. Supposons $q \neq 0$ (ce qui manquait dans l'énoncé). Alors aq^{-1} et $q^{-1}a$ appartiennent à $\mathbb{H}(\mathbb{Q})$ (car $\mathbb{H}(\mathbb{Q})$ est un corps contenant W). D'après ce qui précède, il existe b et b' appartenant à W, tels que $N(aq^{-1} - b) < 1$ et $N(q^{-1}a - b') < 1$

En multipliant par $N(q)$, on obtient : $N(aq^{-1} - b)N(q) < N(q)$ et $N(q)N(q^{-1}a - b') < N(q)$ d'où, compte tenu de A.3.e : $N(a - bq) < N(q)$ et $N(a - qb') < N(q)$.

Il suffit alors de poser $r = a - bq$; $r' = a - qb'$. On a bien $r, r' \in W$ car W anneau.

e) Soit I un idéal à gauche de W, différent de $\{0\}$. Il existe alors dans I un élément non nul, q_0, de norme minimum (c'est possible, car les normes d'éléments de I sont des entiers).

• $q_0 \in I$, donc $Aq_0 \subset I$ (car I idéal à gauche)

• Réciproquement, soit $q \in I$. D'après ce qui précède, il existe $b, r \in W$ tq $q = bq_0 + r$, et $N(r) < N(q_0)$. Or $r = q - bq_0$ et $q \in I$, $bq_0 \in I$, donc $r \in I$.

Par définition de q_0, on a donc $r = 0$; par suite $b = qb_0 \in Aq_0$.

On a donc $I = Aq_0$.

---

3) a) • Relation d'équivalence : évident.

• La classe d'équivalence de x est l'ensemble des $y \in \mathbb{Z}/p\mathbb{Z}$ tels que $y^2 = x^2$.

Or : $y^2 = x^2 \Leftrightarrow (y-x)(y+x) = 0 \Leftrightarrow y = x$ ou $y = -x$ car $\mathbb{Z}/p\mathbb{Z}$ est un corps

D'autre part : $x = -x \iff x = 0$, car $p \geq 3$.

Donc : si $x = 0$, la classe de x est formée de $\{0\}$

si $x \neq 0$, " " " de $\{x, -x\}$.

Or, il est facile de vérifier que l'application $\mathbb{Z}/p\mathbb{Z}/\mathcal{R} \to \mathbb{Z}/p\mathbb{Z}$, $\dot{x} \longmapsto x^2$ est injective ;

il y a donc autant de carrés dans $\mathbb{Z}/p\mathbb{Z}$ que de classes d'équivalences pour $\mathcal{R}$; puisqu'il y a une classe d'éq. à un élément, et $\frac{p-1}{2}$ classes à deux éléments, le nombre de carrés dans $\mathbb{Z}/p\mathbb{Z}$ est $1 + \frac{p-1}{2} = \frac{p+1}{2}$.

b) Le nombre d'éléments de la forme $-a^2$, dans $\mathbb{Z}/p\mathbb{Z}$, est donc $\frac{p+1}{2}$.

Le " " " b^2+1, " , est donc également $\frac{p+1}{2}$.

Les deux ensembles précédents, qui possèdent chacun $\frac{p+1}{2}$ éléments dans $\mathbb{Z}/p\mathbb{Z}$, ont donc nécessairement une intersection non vide. Par suite, il existe a et b, dans $\mathbb{Z}/p\mathbb{Z}$, tels que $-a^2 = b^2+1$. On a donc, dans $\mathbb{Z}$: $b^2 + 1 \equiv -a^2\ [p]$ i.e. a^2+b^2+1 div. par p.

c) Soit $I = \mathbb{W}p + \mathbb{W}(1 + ae_1 + be_2)$

- Soit $q \in I$. Il existe donc x_0, x_1, x_2, x_3, appartenant soit tous à $\mathbb{Z}$, soit tous à $\mathbb{Z} + \frac{1}{2}$, tels que $q = (x_0 p + 1) + (x_1 p + a)e_1 + (x_2 p + b)e_2 + p x_3 e_3$. On a alors

$$N(q) = (x_0^2 + x_1^2 + x_2^2 + x_3^2)p^2 + (2ax_1 + 2bx_2)p + a^2 + b^2 + 1$$

Or : $x_0^2 + x_1^2 + x_2^2 + x_3^2$ est un entier (cf. D.2.b), $2ax_1 + 2bx_2$ est aussi un entier.

Donc $N(q)$ est un entier <u>divisible par p</u>. Les normes des élts de I sont donc toutes divisibles par p, ce qui montre que $I \neq \mathbb{W}$

- $1 + ae_1 + be_2 \notin \mathbb{W}p$ (car les élts de $\mathbb{W}p$ sont de la forme $x_0 p + x_1 p e_1 + \cdots$, avec $(x_0, x_1, x_2, x_3) \in \mathbb{Z}^4$ ou $(x_0, \dots, x_3) \in (\frac{1}{2} + \mathbb{Z})^4$; on ne peut donc avoir $1 = x_0 p$).

Par conséquent $I \neq \mathbb{W}p$.

- D'après D.2.e., il existe $q \in \mathbb{W}$ tel que $I = \mathbb{W}q$.

Or q n'est pas inversible dans $\mathbb{W}$ (sinon, on aurait $I = \mathbb{W}$), donc $N(q) \neq 1$

- Puisque $p \in I = \mathbb{W}q$, il existe $q' \in \mathbb{W}$ tq $p = q'q$. On ne peut avoir $N(q') = 1$, sinon q' serait inversible dans $\mathbb{W}$ et on aurait $q = q'^{-1}p \in \mathbb{W}p$, d'où $I = \mathbb{W}q = \mathbb{W}p$!.

- Par suite, $p = q'q$, donc $N(p) = p^2 = N(q')N(q)$, avec $N(q) \neq 1$, $N(q') \neq 1$.

p étant premier, on a nécessairement $N(q) = p$

d) - si l'élément q précédent appartient à $\mathbb{H}(\mathbb{Z})$, c'est fini

- sinon, on peut écrire q sous la forme $q = 2q_1 + \frac{\pm 1 \pm e_1 \pm e_2 \pm e_3}{2} = 2q_1 + q_2$, avec $q_1 \in \mathbb{H}(\mathbb{Z})$ et $N(q_2) = 1$. En posant $q'' = q\bar{q_2} = q_1(2\bar{q_2}) + 1$, on a $q'' \in \mathbb{H}(\mathbb{Z})$ (car $q_1 \in \mathbb{H}(\mathbb{Z})$ et $2\bar{q_2} \in \mathbb{H}(\mathbb{Z})$) et $N(q'') = N(q)N(\bar{q_2}) = N(q) = p$.

---

4) - Tout nombre premier $p \geq 3$ est somme de 4 carrés d'après ce qui précède. Il en est de même de $p = 2 = 1+1+0+0$, donc de tout produit de nombres premiers d'après 1.c, donc de tout entier.